HOW TO ACHIEVE UK GDPR COMPLIANCE – YOUR QUICK CHECKLIST

You can use this checklist to help build, monitor, and maintain your organization's UK GDPR compliance. Compliance is not a one-time task, but a continuous process that strengthens transparency, security, and customer trust.

Conduct data mapping and maintain records
- Identify what personal data you collect, why you collect it, and who has access.
- Keep records of processing activities and data retention periods.
- Regularly review as staff, systems, and data uses evolve.

Establish lawful bases and consent mechanisms
- Define a lawful basis for each data processing activity.
- Avoid using "legitimate interest" without justification.
- Obtain explicit consent for marketing, analytics, and tracking.
- Keep verifiable records of how and when consent was obtained.

Usercentrics CMP's consent mechanism does not incorrectly use legitimate interest as a lawful basis for data collection and processing.

Implement clear privacy notices
- Publish a transparent, up-to-date privacy notice explaining data use and user rights.
- Display it clearly on your website or app, e.g., privacy policy page.
- Include the date of last update and link to previous versions.

Usercentrics CMP's consent banners inform users about the identities of all third parties with which their information will be shared with if the user grants consent. Users are able to control all information shared with third parties at an individual level.

Manage consent and maintain records
- Obtain valid consent before setting non-essential cookies or trackers.
- Allow easy updates or withdrawals of consent.
- Securely store consent logs (IDs, timestamps, preferences, and versioned consent info.)
- Review consent tools regularly as laws and technologies change.

Usercentrics CMP's consent mechanism makes it as easy to customize consent at a granular purpose level or reject consent as it is to "Accept All." Users are provided with clear information on how to update consent preferences.

It also requires an explicit, affirmative opt-in action from the user before non-exempt storage and access technologies can be set.

Prepare for data subject rights requests
- Be ready to respond to access, correction, deletion, or portability requests within one month.
- Know where data resides across systems.
- Automate where needed to handle larger request volumes efficiently.

Secure data and assess risk
- Apply encryption, access controls, and continuous monitoring.
- Conduct Data Protection Impact Assessments (DPIAs) for high-risk processing.

Train teams and assign responsibilities
- Provide regular UK GDPR and data security training tailored to employee roles.
- Designate a Data Protection Officer (DPO) if required.
- Promote a culture of privacy awareness across all departments.

Tip: Review this checklist quarterly or after any major system, product, or regulatory change to keep your privacy compliance current.